

Received  
FEB 10 1997



172 #5  
**Secure Computing  
Corporation**

2675 Long Lake Road  
Roseville, MN 55113  
U.S.A.

Phone: (612) 628-2700  
Fax: (612) 628-2701

EEO/AA

February 3, 1997

Nancy Crowe  
Regulatory Policy Division  
Bureau of Export Administration  
Department of Commerce  
14th Street and Pennsylvania Ave., N.W.  
Room 2705  
Washington, D.C. 20230

Re: Comments to Interim Rules - Bureau of Export Administration,  
15 CFR 730, et seq.  
Comment Date: February 13, 1997

Dear Ms. Crowe:

Pursuant to 61 Federal Register 68573, dated December 30, 1996, we have the following comments to make to the proposed interim rules affecting encryption items transferred from the U.S. Munitions List to the Commerce Control List. Specifically, our comments address Supplement No. 4 to Part 742 -- Key Escrow or Key Recovery Products Criteria.

In paragraph (6), "Interoperability Feature" the proposed subsection (i) reads as follows:

- (i) Other key recovery products that meet these criteria, and shall not interoperate with products whose key recovery feature has been altered, bypassed, disabled, or otherwise rendered inoperative;

It is not technically feasible for a local key recovery product to determine if the remote key recovery product has been tampered with. The local key recovery product cannot anticipate and detect all the possible ways the remote device could have been altered. In addition, it is not possible for products produced today to anticipate how future products will operate and how they could be altered.

The intent of this requirement appears to be that, a (local) key recovery product shall not interoperate with other products if such operation would impair the Government's ability

Nancy Crowe  
February 3, 1997  
Page 2

to obtain the key(s) for data exchanged (both directions) between the communicating products.

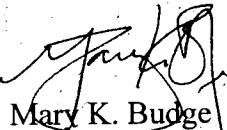
We request consideration that paragraph (6)(i) be rewritten as follows:

(i) Other key recovery products that meet these criteria, and shall not interoperate with products whose key recovery feature has been altered, bypassed, disabled, or otherwise rendered inoperative such that it would impair the Government's ability to obtain the key(s) for data exchanged (both directions) between the communicating products;

The advantage of the revised wording is that it clearly states the requirement that the government must be able to obtain the keys necessary to decrypt all the data. It also would eliminate the need for developers to build systems which anticipate and detect tampering by the remote device.

Thank you for considering the proposed change. Please do not hesitate to contact me should you have any questions regarding the above.

Sincerely,



Mary K. Budge  
Contracts Counsel  
Secure Computing Corporation  
2675 Long Lake Road  
Roseville, MN 55113  
(612)628-6221